UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

EVAN SAURAY, on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. ARDEN CLAIMS SERVICE LLC, Defendant.	**CASE NO. 24-cv-645** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff EVAN SAURAY ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant ARDEN CLAIMS SERVICE LLC ("Arden" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names and Social Security numbers ("personal identifying information" or "PII").

3. Arden's breach differs from typical data breaches because it affects consumers who had no relationship with Arden, never sought one, and never consented to Arden collecting and storing their information.

4. On information and belief, the Data Breach was discovered on October 17, 2023. Due to Defendant's obfuscating language, it is unclear how long the cybercriminals had unfettered access to the Plaintiff's and the Class's private information before Defendant finally discovered the Breach.

5. On January 17, 2024, Arden finally notified state Attorneys General and many putative Class Members about the widespread Data Breach ("Notice Letter"). Plaintiff's Breach Notice is attached as **Exhibit A.** A Sample Notice Letter is attached as **Exhibit B**. Arden waited three months before informing Class Members about the Data Breach, even though Plaintiff and a staggering 50,032 Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. Arden's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened on Arden's systems, or why it took Arden three months to begin notifying victims that hackers had gained access to highly personal PII.

7. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former consumers.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Evan Sauray is a Data Breach victim.

12. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Evan Sauray, is a natural person and citizen of New York, where he intends to remain.

14. Defendant, Arden, is a New York company with its principal place of business at 322 Main St, Port Washington, NY 11050.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one member of the class is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Arden

18. Arden advertises itself as an "executive team with years of professional experience as arbitrators, mediators, attorneys, and accountants" who utilize "state-of-the-art technology and secure processes that expedite and simplify the Claims Administration process."[1] Arden further touts itself as being "committed to providing personal, comprehensive and efficient service to your settlement administration process".[2] Arden boasts a total annual revenue of $6.1 million.[3]

19. Arden's services are specialized for companies who oversee highly sensitive data. Arden thus must oversee, manage, and protect the PII of its clients' consumers, Arden's consumers.

20. On information and belief, these third-party consumers, whose PII was collected by Arden, do not directly do any business with Arden.

21. As a self-proclaimed leader in its industry handling highly sensitive aspects of its clients' business, Arden understood the need to protect consumers' data and prioritize its data security.

[1]Arden, https://ardenclaims.com/about-arden-claims-service/ (last visited January 24, 2024).
[2] *Id.*
[3]Arden, Zoominfo, https://www.zoominfo.com/c/arden-claims-service-llc/399380674 (last visited January 24, 2024).

22. Indeed, Arden not only boasts that it utilizes state of the art technology and secure processes, but also states that it "invested significant resources on maintaining stringent security practices to ensure the highest levels of data protection measures for our clients."[4]

23. Despite recognizing its duty to do so, on information and belief, Arden has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Arden leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

24. Plaintiff is unsure how Arden got his information but assumes a company utilizing Arden's settlement administrator services provided Arden with his PII, including but not limited to his name, and Social Security Number.

25. On information and belief, Defendant collects and maintains consumers' PII in its computer systems.

26. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

27. According to the Breach Notice, on October 17, 2023, Arden noticed "suspicious activity within our computer network environment." Ex. A. Following an internal investigation, Arden discovered that there had been "unusual activity related to an email account." Following an internal investigation, Arden admits that "an unknown actor acquired certain data without authorization." Ex. A.

[4]Why Arden Claims, Arden, https://ardenclaims.com/why-arden-claims-service/ (last visited January 24, 2024).

28. In other words, Arden's investigation revealed that its cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private PII.

29. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

30. Additionally, Defendants admitted that PII was actually stolen during the Data Breach confessing that the information was not just accessed but was "acquired" from its system. Ex. A.

31. On or around January 17, 2024 –three months after the Breach first occurred – Arden finally notified Plaintiff and Class Members about the Data Breach.

32. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

33. In response to the Data Breach, Defendant contends that it has "implemented additional security measures." Ex. A. Although Defendant fails to expand on what these alleged "security measures" are, such measures should have been in place before the Data Breach.

34. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords." Defendant further encouraged breach victims to "promptly report any fraudulent activity or any suspected incidence of identity theft." Ex. B.

35. Defendant further recognized through its Breach Notice, its duty to implement reasonable cybersecurity safeguards or policies to protect its consumers' PII, promising that, despite the Data Breach demonstrating otherwise, it "takes the privacy and security of your information very seriously" and that "[t]he privacy and security of personal information is a top priority for Arden Claims Service." Ex. B.

36. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

37. On information and belief, Arden has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

38. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

40. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's

negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

41. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in its industry preceding the date of the breach.

42. In light of recent high profile data breaches, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

43. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

44. Indeed, cyberattacks against Defendant's industry has become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[7]

---

[5] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).

[6] *Id*.

[7] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).

45. Cyberattacks on companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

46. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Arden.

Plaintiff's Experience

47. Plaintiff Sauray received Arden's Breach Notice in or around January 2024.

48. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for three months.

49. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

50. Plaintiff does not recall ever learning that his PII was compromised in a data breach incident, other than the breach at issue in this case.

51. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring him accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

[8] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

52. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

53. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

54. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

55. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

56. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

57. Indeed, following the Data Breach, Plaintiff has experienced an enormous increase in spam calls, many of which utilize international cell phone numbers, suggesting that his PII is now in the hands of cybercriminals.

58. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised

to gather and steal even more information.[9] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

59. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

60. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

61. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

[9] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

62. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

63. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

64. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

65. One such example of criminals using PII for profit is the development of "Fullz" packages.

66. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

67. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

68. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

69. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

70. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued

numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

71. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

72. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

73. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

76. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

77. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

78. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

79. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

81. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Arden Data Breach including all those who received notice of the breach.

82. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

83. Plaintiff reserves the right to amend the class definition.

84. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least 50,032 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

   i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

   ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

   iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

   iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

   v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

   vi. Whether Defendant's Breach Notice was reasonable;

   vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

85. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

86. Plaintiff realleges all previous paragraphs as if fully set forth below.

87. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

88. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

89. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

90. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII.

91. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII.

92. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

94. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

95. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

96. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII.

97. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII.

98. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

99. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII —whether by malware or otherwise.

100. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

101. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

102. Defendant breached these duties as evidenced by the Data Breach.

103. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

104. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

105. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

106. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

107. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including

monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

108. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and the Class)

109. Plaintiff realleges all previous paragraphs as if fully set forth below.

110. Defendant entered into various contracts with its clients to provide settlement administration services to its clients.

111. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

112. Defendant knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

113. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

114. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

115. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

116. Plaintiff realleges all previous paragraphs as if fully set forth below.

117. Plaintiff and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

118. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate its services to Plaintiff and the Class.

119. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

120. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

121. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's PII because Defendant failed to adequately protect their PII.

122. Plaintiffs and Class Members have no adequate remedy at law.

123. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT IV
Violation Of The New York Deceptive Trade Practices Act ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges all previous paragraphs as if fully set forth below.

125. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' PII;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' PII;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

126. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the Class Members' PII entrusted to it, and that risk of a data breach or theft was highly likely.

127. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

128. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendant's network and aggregation of PII.

129. The representations upon which consumers (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of PII), and current and former employees (including Plaintiff and Class Members) relied on those representations to their detriment.

130. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members have been harmed,

in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

131. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

132. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing employment benefit services to consumers in the State of New York. 167.

133. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

134. Plaintiff and Class Members were injured because:

a. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and

b. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

135. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and the Class Members suffered damages including, but not limited to: (i) lost or diminished value of their PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;

(iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) damage to his credit score; and (vi) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

136. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

137. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

138. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

139. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

140. Also as a direct result of Defendant's violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: January 29, 2024,

Respectfully submitted,

By: /s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Tel: (212) 558-5500
jbilsborrow@weitzlux.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class